UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 7
Issue 1 *Fall 2005*

Article 20

10-1-2005

The Seamy Side of the Seamy Side: Potential Danger of Cyberpiracy in the Proposed .xxx Top Level Domain

Jennifer D. Phillips

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 7, ISSUE 1: FALL 2005

Editor's Note: *In Volume 6, Issue 1 of the North Carolina Journal of Law and Technology, Kate Reder published an article on a related topic, entitled "Ashcroft v. ACLU: Should Congress Try, Try, and Try Again, or Does the International Problem of Regulating Internet Pornography Require an International Solution?" 6 N.C. J. L. & TECH. 139 (2004). In that article the author discussed the .xxx domain as one of possible solution to filtering software or Congressional regulation. The following article takes the subject one step further, discussing the legal ramifications for adult entertainment companies who become engaged in a domain dispute involving a .xxx tag.*

THE SEAMY SIDE OF THE SEAMY SIDE: POTENTIAL DANGER OF CYBERPIRACY IN THE PROPOSED ".XXX" TOP LEVEL DOMAIN

Jennifer D. Phillips[1]

Recently, the Internet Corporation for Assigned Names and Numbers ("ICANN") has considered a proposal which would create a top level domain ("TLD") exclusively for sexually oriented adult content, called ".xxx." The proposal for the TLD outlines registration steps to protect trademark holders, individuals, and mainstream businesses from cyberpiracy, yet all but ignores the possibility of cyberpiracy within the adult entertainment community. Without registration safe guards, adult entertainment providers can only protect themselves against cyberpiracy by utilizing ICANN arbitration and federal cyberpiracy law, which tend to not apply well in the adult entertainment context. This comment examines how the .xxx proposal does not protect adult entertainment websites and explains why litigation and arbitration do not adequately protect adult entertainment websites against cyberpiracy within the proposed .xxx.

---

[1] J.D. Candidate, University of North Carolina School of Law, 2007. Special thanks to my brother Bill for helping me find a topic and to Timothy J. Duva for helping me research Internet technology.

I. INTRODUCTION

In a rare "hell freezes over" scenario, conservative Christian groups might be the saving grace of adult entertainment. Recently, and largely because of the intervention of the Bush administration, the Internet Corporation for Assigned Names and Numbers ("ICANN") has put the proposed .xxx top level domain ("TLD") on hold. For perhaps the first time ever, Christian groups and business-savvy adult entertainers are in agreement on something pertaining to pornography: the .xxx domain is a bad idea. Obviously, the reasoning behind their respective opinions differs greatly. Conservative Christian groups have been extremely vocal about their concerns, claiming that the domain will legitimize online pornography and fail to protect children.[2] Although less openly vocal about their concerns,[3] adult entertainment companies are concerned with possible negative effects the TLD could have on their businesses, particularly when they have spent time and money developing a customer base on a different TLD.[4] Perhaps what is most interesting is that the groups represent the most extreme positions of their respective view points. Many moderate to conservative Christians believe that the .xxx TLD is desirable, as it will be easier to filter, thus preventing children from accessing sexually explicit sites. On the other side of the fence, many adult

---

[2] "Horrid pornography is about to be honored with a permanent home on the Internet by the Department of Commerce, which is expected to approve .XXX domains." ConservativePetitions.com, http://www.conservativepetitions.com/petitions.php?id=E4306 (last visited Nov. 6, 2005) (on file with the North Carolina Journal of Law & Technology).

[3] Christian organizations have reported sending over 6000 letters to President Bush asking him to stop the approval of the .xxx TLD. A rampant and persistent rumor on the Internet is that many of these "Christians" were actually pornographers in disguise. For an example of this rumor, see CircleID, http://www.circleid.com/posts/xxx_puzzle_pieces_start_to_come_together_and_the_picture_is_ugly/ (last visited Nov. 6, 2005) (on file with the North Carolina Journal of Law & Technology).

[4] *See* Jim Wagner, Will Webmaster Move to .xxx?, Internetnews.com, June 3, 2005, http://www.Internetnews.com/xSP/article.php/3510056 (last visited Oct. 13, 2005) (on file with the North Carolina Journal of Law & Technology).

entertainment companies anticipate the marketing benefits the new .xxx domain will provide.[5]

A common reservation voiced by all groups, however, is the potential abuse of the TLD by cyber- and typosquatters. A problem that, to this point, legislation has been unable to sufficiently address, cyber- and typosquatting crime emerged in the 1990's with the rise of the Internet. Cybersquatting developed first, and has received a good deal of mainstream attention.[6] Simply put, cybersquatting involves buying a domain name that is of interest to an established person, business, or organization.[7] The cybersquatter then either tries to sell the domain name to the interested party at a greatly inflated price, or keeps the name and directs all traffic to another, often unrelated website.[8] Commonly, these crimes go together, with the hijacked name directing traffic to a website containing antisocial content in an attempt to coerce the owner into paying a ransom for the domain name.[9] Typosquatting is a related, although separate, issue. Generally, it involves "misspelling or variations of legitimate domain names in

---

[5] *Id.*

[6] See John D. Mercer, Cybersquatting: Blackmail on the Information Superhighway, 6 B.U. J. SCI. & TECH. L. 11, 13 (2000).

[7] The World Intellectual Property Organization ("WIPO") defines cybersquatting as "the deliberate, bad faith abusive registration of a domain name in violation of rights in trademarks and service marks." The Management of Internet Names and Addresses: Intellectual Property Issues, World Intellectual Prop. Org. 53-54 (Apr. 30, 1999), http://arbiter.wipo.int/processes/process1/report/pdf/report.pdf (last visited Oct. 13, 2005) (on file with the North Carolina Journal of Law & Technology).

[8] *Id.*

[9] *See, e.g.*, Parisi v. Netlearning, Inc., 139 F. Supp. 2d 745 (E.D. Va. 2001). Parisi lawfully obtained the rights to netlearning.com. *Id.* at 746. When a business named Netlearning, Inc. contacted Parisi to arrange a transfer of the name, Parisi alleges that Netlearning offered $22,500 for the rights to the website, which was about 1000 times more than Parisi originally paid. *Id.* at 748. Parisi rejected the offer, and Netlearning responded by initiating an UDRP administrative proceeding. *Id.* In retaliation Parisi linked netlearning.com to a website called whitehouse.com, which specialized in doctored photos of first ladies engaging in sexual acts with first pets. For a full discussion of this case, *see* Chad Emerson, Wasting Time In Cyberspace: The UDRP'S Inefficient Approach Toward Arbitrating Internet Domain Name Disputes, 34 U. BALT. L. REV. 161, 176-79 (2004).

order to trick individuals into viewing unrelated advertisements or web sites."[10] While not all typosquatting is done with criminal intent,[11] it often directs Internet users to pornographic websites. Because minors use the Internet,[12] some legislation has been passed to prevent typosquatting.[13] For the purposes of this article, "cyberpiracy" will refer to both cybersquatting (problematic when a trademark is infringed), and typosquatting (problematic when a trademark is infringed or diluted, but rising to a level of a crime when minors are endangered.)[14] In addition to cyberpiracy, there are also concerns involving domain disputes, where two or more legitimate businesses or people have interest in the same domain name.

Because cyberpiracy is often associated with pornography and adult content, the proposed .xxx TLD has led to great concerns among Internet users and domain name owners. A survey of any website with a forum dedicated to the proposed .xxx TLD will find speculations on worst-case cybersquatting scenarios, where every decent citizen who does not want his or her name or company associated with pornography must preemptively buy an .xxx domain name. From a legal perspective, most of these concerns are unfounded. The proposed registration process in the .xxx TLD

---

[10]Christopher G. Clark, Note, *The Truth in Domain Names Act of 2003 and A Preventative Measure to Combat Typosquatting*, 89 CORNELL L. REV. 1476, 1488 (2004).

[11]For instance, "cybergriping," a form of typosquatting that involves the use of misspelled corporate domain name, is done with the intent to complain about the company in question. "Cybergriping" has been considered by some courts to be protected speech under the First Amendment. For a full discussion on cybergriping, *see* Hannibal Travis, The Battle for Mindshare: the Emerging Consensus that the First Amendment Protects Corporate Criticism and Parody on the Internet, 10 VA J.L. & TECH. 3, 2005, http://www.vjolt.net/vol10/issue1/v10i1_a3-Travis.pdf (last visited Nov. 18, 2005) (on file with the North Carolina Journal of Law & Technology).

[12]See Clark, *supra* note 10, at 1505. For a complete discussion of how typosquatting negatively impacts children, *see* Susan Hanley Kosse, Try, Try Again: Will Congress Ever Get It Right? A Summary of Internet Pornography Laws Protecting Children and Possible Solutions, 38 U. RICH. L. REV. 721 (2004).

[13]Clark, *supra* note 10 at 1505

[14]Travis, *supra* note 11 at 3.

application[15] outlines a set of steps designed to prevent cybersquatting and typosquatting.[16] If implemented as proposed, the steps should provide adequate protection for those who are not a part of the adult entertainment industry. Furthermore, federal law will provide adequate relief for those mainstream businesses and individuals who are victimized by any opportunistic cyberpirate who manages to slip by the strict registration procedure.

Ironically, the .xxx cyberpiracy will not threaten unwitting web-surfers with unexpected and offensive online pornography, as has traditionally been the case, nor will it hold hostage desirable domain names sought by mainstream businesses or individuals.[17] Rather, the potential victims of .xxx cyberpiracy are adult entertainment companies, including the same adult entertainment companies whose aggressive marketing tactics wreaked havoc in the .com, .net, and .org domains. The domain registration screening protections proposed by ICM are explicitly denied to adult entertainment websites. The procedures are designed to protect only legitimate businesses from exploitation in the .xxx TLD.[18] Under the proposal, adult entertainment companies are ostensibly protected from mainstream businesses, though the threat posed to adult entertainment by mainstream businesses is minimal.[19]

---

[15]The application is submitted to ICANN, the organization with the power to approve or reject TLD applications.

[16]See .xxx New TLD RFP Application, http://www.icann.org/tlds/stld-apps-19mar04/xxx.htm (last visited October 12, 2005) [hereinafter .xxx Application] (on file with the North Carolina Journal of Law & Technology).

[17] A reading of the .xxx new TLD RFP Application reveals that all measures taken to ensure secure registration are aimed at mainstream businesses, trademark holders, and individuals, not adult entertainment sites. *Id.*

[18] *Id.*

[19] In its application to ICANN, ICM reasons that "there are likely not going to be many non-adult entertainment companies trying to establish a presence online in an adult oriented TLD, as they would be prohibited by the charter criteria anyway. Although there may be some entities that may try to extort money from existing adult-entertainment companies, ICM and [IF]FOR believe that the modified STOP proceeding and other IP safeguard mechanisms adequately address these concerns." *Id.* at Policy Making Process § C(2). Whether or not

Unshielded by ICM, adult entertainment companies will be vulnerable to all varieties of cyberpiracy and subject to multiple domain name disputes. Compounding this problem is the fact that laws and proceedings designed to deal with cyberpiracy and domain disputes are entrenched in trademark law. What have been workable legal solutions in other contexts will not function correctly in the .xxx context. Many of the names registered will be generic terms that cannot be trademarked.[20] Another group potentially affected includes small sites whose names are not well known enough to warrant trademark registration.[21] Up until now, they may have been confident in the fact that they owned the right to their domain name. However, the .xxx domain creates a situation where a competitor can buy an identical domain name, potentially deflecting customers from the original site. Because neither group owns a registered trademark, trademark law will prove inadequate to protect these groups.

II. INTERNET TERMINOLOGY FOR THE TECHNOLOGICALLY DISINCLINED

When trying to place domain disputes in context, a basic knowledge of the Internet and Internet jargon is invaluable. The traditional definition of the "Internet" is a "worldwide network of interconnected computers, all of which use a common protocol . . . to communicate with each other."[22] The "World Wide Web" is made up of Web pages, which we access on the Internet and which are written in a computer code called Hypertext Mark Up

---

the STOP proceedings and IP safe guards actually address these problems is discussed *infra* Parts IV, V.

[20] Zatarains v. Oak Grove., 698 F2d 786 (5th Cir. 1983) (holding that descriptive terms cannot ordinarily be trademarked).

[21] *See id.* (holding that sometimes descriptive terms can be trademarked if they are so well known that public attributes to them a secondary meaning). It is unlikely, however, that a small pornography site will be so well known that its descriptive terms will give rise to trademark protection.

[22] *See, e.g.*, Boutell.Com, WWW FAQs: What are HTML and XHTML?, http://www.boutell.com/newfaq/definitions/html.html (last visited Nov. 7, 2005) (on file with the North Carolina Journal of Law & Technology).

Language ("HTML").[23] Every webpage has an address, which is a number assigned by ICANN.[24]

Because most people cannot remember long strings of numbers, "domain names" are used to identify websites. Most domain names consist of three parts which identify the website.[25] The "www" portion indicates the page is available on the World Wide Web. The domain name is the name by which the site is commonly identified (i.e., the "amazon" in amazon.com.) The suffix of the domain name is the TLD. Familiar examples of these include .com, .net., .gov, and .org.[26]

ICANN is a non-profit corporation and the only organization authorized to assign domain names, though they typically delegate this authority to companies who are capable of handling an entire TLD. This article is concerned with the creation of a new .xxx TLD, which would be dedicated to the adult entertainment industry. The company that has proposed .xxx is ICM registry ("ICM"), a corporation formed expressly for that purpose. Although negotiations between ICM and ICANN are well past the preliminary stages, the domain is currently on hold.[27]

---

[23] *Id.*

[24] ICANN.org, ICANN information: What is the domain name system?, http://icann.org/general/general. (last visited November 2, 2005) (on file with the North Carolina Journal of Law and Technology).

[25] *Id.*

[26] Boutell.com, WWW FAQs: What is the domain name?, http://www.boutell.com/newfaq/definitions/domainname.html (last visited Nov. 21, 2005) (On file with the North Carolina Journal of Law and Technology).

[27] The official reasons that ICANN decided to place the TLD on hold are available on the ICANN website. *See* ICANN, Special Meeting of the Board: Preliminary Report, Sept. 15, 2005, http://www.icann.org/minutes/ resolutions-15sep05.htm (last visited Oct 30, 2005) (on file with the North Carolina Journal of Law and Technology). However, many have speculated that the primary reason for deferral was the request of the White House, acting under pressure from the Family Research Council. *See* Wendy Cloyd, XXX Internet Domain Name on Hold, CitizenLink, Aug. 17, 2005, http://www.family.org/cforum/feature/a0037572.cfm (last visited October 13, 2005) (on file with the North Carolina Journal of Law and Technology).

III. LAWS RELATING TO CYBERPIRACY AND DOMAIN NAME DISPUTE

Although the federal government recognized cyberpiracy as a problem as early as the mid 1990s, it has yet to come up with a satisfactory method of resolving domain name disputes. Most legislation in this area has centered around cybersquatting, with some of it touching on areas of typosquatting. Domain name disputes not involving cyberpiracy are common, but are not specifically addressed by any legislation.[28]

Parties involved in a cyberpiracy case or domain dispute can choose to litigate under federal law, or pursue alternative dispute resolution through ICANN's Uniform Dispute Resolution Policy ("UDRP").[29] According to numerous legal commentators, the general problems with both the federal legislation and the UDRP involve an inability to reach all claims and charges that seem deserving of protection, and a lack of a clear, consistent standard by which claims and charges may be adjudicated and an inadequate punishment of offenders.[30]

---

[28]Domain name disputes for smaller businesses and website owners are typically handled by ICANN's Uniform Dispute Resolution Policy ("UDRP"). While proceeding under the UDRP has certain advantages (i.e. litigation can be resolved within forty-five days), at least one commentator has opined that the UDRP really represents a "separate and unequal" means of dispute for the smaller website owner. See Travis, *supra* note 11, at 31-32.

[29]ICANN, Uniform Domain Name Dispute Resolution Policy, Oct. 24, 1999, http://www.icann.org/udrp/udrp-policy-24oct99.htm (last visited October 13, 2005) [hereinafter UDRP] (on file with the North Carolina Journal of Law & Technology).

[30]*See* Clark, *supra* note 10; Emerson, *supra* note 9; J. Ryan Gilfoil, *A Judicial Safe Harbor Under the Anti-Cybersquatting Consumer Protection Act*, 20 BERKELEY TECH L.J. 185 (2005); J.R. Hildenbrand, Comment, *A Normative Critique of Private Domain Name Dispute Resolution*, 22 J. MARSHALL J. COMPUTER & INFO.L. 625 (2004); Mercer, *supra* note 6; Travis, *supra* note 15; Minqin Wang, Note, *Regulating the Domain Name System: Is the ".BIZ" Domain Name Distribution Scheme an Illegal Lottery?*, 2003 U. ILL. L. REV. 245 (2003).

A. *The Federal Trademark Dilution Act and the Lanham Act*

Perhaps more than any other technological development, the Internet poses unique and unanticipated legal problems. Having realized the importance of the Internet before much of corporate America, early cybersquatters bought numerous valuable domain names and essentially held them hostage. At the time,[31] trademark law seemed most closely analogous to the problems presented,[32] so lawyers pursued claims under the Lanham Act,[33] specifically under the Federal Trademark Dilution Act[34] ("FTDA")[35] provision of the act. Despite the inadequacy of these laws and the difficulty of applying them in a domain dispute context, these two statutes remain viable causes of action today and have influenced much of the subsequent cyberpiracy legislation.[36]

---

[31]The earliest cybersquatting cases involved plaintiffs such as MTV, which held universally famous trademarks. Trademark infringement was a good option, because the crime literally did involve the infringement of a trademark. This has not been true of all cybersquatting cases. *See, eg*, inventionpatent.net, *available at http*://www.inventionpatent.net/trademark/trademark-domain-name-5.cfm.

[32]Some have suggested that trademark infringement has never been a good analogy for domain disputes. Unlike a trademark, "the current [domain name system] DNS requires that each second-level domain name in any given TLD be unique. This uniqueness requirement is fundamentally inconsistent with the coexistence of identical trademarks. While trademark law permits multiple parties to use the same mark for different products or services, or within different geographical areas, the gTLDs uniqueness requirement applies globally and in all markets." Wang, *supra* note 30, at 251.

[33]15 U.S.C. § 1114 (2000).

[34]15 U.S.C. § 1125 (2000) (commonly referred to as § 43(a) of the Lanham Act or the Federal Trademark Dilution Act).

[35]*See* Clark, *supra* note 10, at 1493.

[36]"When courts were first asked to decide the legitimacy of cybersquatting, plaintiffs brought claims alleging FTDA violations. Although the FTDA claims were buttressed with other claims, e.g., ordinary trademark infringement and unfair competition, some courts decided that since the FTDA could solve the problem it was unnecessary to address the other claims. Unfortunately, by trying to quickly address the cybersquatting problem, these courts have stretched the applicability of the FTDA beyond its intended borders. [Thus, c]ourts have created precedents that are inclined to unfairly favor plaintiffs and cause more harm than good." Mercer, *supra* note 6, at 297-98.

In applying trademark law to domain name disputes, two significant problems arise. First, in following with the traditions of trademark law, the Lanham Act "does not apply well in cybersquatting cases because it requires a showing of the likelihood of consumer confusion."[37] Originally, this provision of the Act was construed very broadly in the Internet context. Courts established law that virtually any time an Internet user could spend at the wrong site would satisfy the consumer confusion requirement.[38] As the Internet developed, the judiciary realized this was an unrealistic application of the law, and the courts shifted towards a reading of the statute that required actual customer confusion.[39] While the more recent construction of the statute tends to result in outcomes that seem more fair, it also limits the scope of the Act in terms of the Internet. Specifically, the law applies well in those cases in which the cybersquatter has registered the domain name in hopes of benefiting from the goodwill accrued by another person or business.[40] However, the recent bulk of the cybersquatting cases involved domain names that are not actually in use or are used in such drastically different ways that customer confusion is highly unlikely.[41]

In response to this problem, Congress eliminated the "likelihood of customer confusion" element of the statute in hopes of creating more causes of action for cybersquatting cases.[42] However, the "commercial use" provision of the FTDA was retained. Cyberpirates, an ever innovative and opportunistic group, quickly adapted. They could avoid legal consequences by

---

[37]Wang, *supra* note 30, at 253.

[38]Travis, *supra* note 11, at 23.

[39] In *Planned Parenthood Fed'n of Am., Inc. v. Bucci*, the court disregarded the content in considering customer confusion. *Planned Parenthood Fed'n of Am., Inc. v. Bucci*, 1997 U.S. Dist. LEXIS 3338, No. 97 Civ. 0629, 1997 WL 133313 (S.D.N.Y. March 24, 1997), aff'd, 152 F.3d 920 (2d Cir. 1998). More recently, other circuits have explicitly rejected this holding: the case was "wrongly decided to the extent that in determining whether the domain names were confusing, the courts did not consider whether the websites' content would dispel any confusion." Lamparello v. Falwell, 420 F.3d 309, 318 (4th Cir. 2005).

[40] Wang, *supra* note 30 at 253.

[41]*Id.*

[42]*Id.* at 254.

either not using the domain names at all or by using them for noncommercial purposes, thus rendering the statute virtually meaningless.[43] As one court remarked:

> In cases of warehousing and trafficking in domain names, courts have sometimes declined to provide assistance to trademark holders, leaving them without adequate and effective judicial remedies. This uncertainty as to the trademark's application to the Internet has produced inconsistent judicial decisions and created extensive monitoring obligations, unnecessary legal costs, and uncertainty for consumers and trademark owners alike.[44]

B. *Anticybersquatting Consumer Protection Act*

By the late 90's, it was clear that the FTDA alone was not adequate for cybersquatting cases. Some sort of legislation was necessary to actually prevent and punish cyberpiracy. In 1999, the congressional solution to the problem was the Anticybersquatting Consumer Protection Act ("ACPA").[45] While an improvement over the FTDA, the ACPA has also proven to be too limited in scope to reach all of the intended abusive domain name registrations that it endeavored to prevent and punish.

A definitive characteristic of the ACPA is that it protects only trademark holders and those who register their personal names as domain names. This is great for individual registrants and trademark holders who are victims of cyberpiracy,[46] but the statute leaves nearly everyone else without a legal remedy.[47]

---

[43]Clark, *supra* note 10, at 1496.

[44]Victoria's Cyber Secret Ltd. P'ship v. V Secret Catalog, Inc., 161 F. Supp. 2d 1339, 1346 (S.D. Fla. 2001) (quoting S. Rep. No. 106-140, at 7 (1999)).

[45]15 U.S.C. § 1125(d) (2000).

[46] Wang, *supra* note 30, at 253. In Schmidheiny v. Weber, 285 F. Supp. 2d 613 (E.D. Pa. 2003), defendant Weber was found to have registered hundreds of domain names correlating to well known, wealthy individuals, including Schmidheiny. *Id.* at 618-20. Weber attempted to sell the domain name back to Schmidheiny for over one million dollars. *Id.* at 618. Summary judgment granted under the Anticybersquatting Consumer Protection Act (ACPA) are based on the facts presented. *Id.* at 628.

[47]Clark, *supra* note 10, at 1497 (quoting Ford Motor Co. v. Greatdomains.com, Inc., 177 F. Supp. 2d 635, 642 (E.D. Mich. 2001)).

The other problematic characteristic of the ACPA is that it requires bad faith intent as the statute was drafted to "target individuals who register domain names solely to 'profit by extortion.'"[48] The statute sets down nine possible factors that could lead to a finding of bad faith.[49] However, "in determining bad faith intent, the Court may consider all relevant factors and is not limited to the nine listed factors in determining whether or not the bad faith criteria [sic] has been met."[50] Furthermore, "the court is free to assign to the factors any relative weight it chooses."[51] While seemingly well tailored to target a particular aspect of cyberpiracy, the ACPA also provides a broad safe harbor provision. Essentially, anyone who can prove that they have a legitimate business interest in the domain name may have an affirmative defense to the ACPA.[52] Some legal commentators have argued that this safe harbor provision is so broad that, in effect, the ACPA reaches only the most egregious, extortion related cybersquatting cases.[53]

From the standpoint of victims of cyber crime, the ACPA was an improvement over the FTDA and Lanham Act. For all others embroiled in domain disputes, the statute remained a side note in a frustrating legal process.

---

[48] Clark, *supra* note 10, at 1496 (2004), quoting *Ford Motor Co. v. Greatdomains.com, Inc.*, 177 F. Supp 2d 635, 642 (E.D. Mich. 2001).

[49] *See* 15 U.S.C. 1125(d)(1)(B) (2000). To paraphrase, the factors include: (I) the intellectual property rights of the domain name, (II) whether the domain name is a legal name of a person or business, (III) the person's prior use of the domain name, (IV) the fair use of the mark, (V) the intention to divert customers from the mark owner or to tarnish the mark owner's reputation, (VI) the person's offer to sell the domain to the mark owner for a financial gain without having used the domain name commercially, (VII) the provision of false contact information in registering the domain, (VIII) the acquisition of multiple names that may be similar to a distinct mark, (IX) and the extent to which the registration is or is not distinctive. *Id.*

[50] Victoria's Cyber Secret Ltd. P'ship v. V Secret Catalog, Inc., 161 F. Supp. 2d 1339, 1347 (S.D. Fla. 2001).

[51] Gilfoil, *supra* note 30, at 189 (2005).

[52] Clark, *supra* note 10, at 1498.

[53] For an in-depth criticism of federal anti-cyberpiracy legislation, *see* Hildenbrand, *supra* note 30.

C. *Uniform Dispute Resolution Policy*

In 1999, ICANN implemented its Uniform Dispute Resolution Policy, which lays out a set of guidelines for alternative dispute resolution.[54] Originally, the UDRP was meant to be an efficient, economic alternative to cyberpiracy litigation under state and federal law.[55] However, like federal cyberpiracy legislation, the UDRP is married to the principles of trademark law.[56] Thus, it has been widely argued that UDRP has "permitted the divestment of [the domain name owner's] rights in summary fashion under 'procedures that have systematically favored intellectual property owners even in doubtful cases.'"[57] On the other hand, it has been suggested that when neither party possesses a trade or service mark, the arbitrations tend to end in convoluted, arbitrary, and murky decisions, with all parties denied adequate protection under the law.[58]

While aligning itself with federal laws in some regards, the UDRP differs from the federal laws in several important ways, the most glaring of which is the policy's definition of bad faith. Specifically, the policy outlines three factors the complainant must prove: (1) the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; (2) the defendant has no rights or legitimate interests with respect to the domain name; and (3) the defendant's domain name has been

---

[54]UDRP, *supra* note 29.

[55]There is a school of thought that resolving the domain name dispute under the UDRP is more expensive than federal litigation. *See* Emerson, *supra* note 9.

[56]Although frequently called upon to apply trademark law or deal with trademark disputes, more than one commentator has noted that "UDRP panels are simply not designed to handle trademark infringement cases, which are often factually intensive and which may turn on critical issues like freedom of speech." Travis, *supra* note 11, at 34 (quoting Delta Air Transport NV v. De Souza, WIPO Case No. D2003-0372 (Aug. 5, 2003), at Dissent, *http*://arbiter.wipo.int/domains/decisions/html/2003/d2003-0372.html) (last visited Nov. 18, 2005) (on file with North Carolina Journal of Law and Technology).

[57]*Id.* at 31-32 (quoting A. Michael Froomkin & Mark A. Lemley, ICANN and Antitrust, 2003 U. ILL. L. REV. 1, 68 (2003)).

[58]For an in depth discussion of the inadequacies of the UDRP, *see* Emerson, *supra* note 9.

registered and is being used in bad faith.[59] Section 4b defines bad faith.[60] As concerned service providers, such as AOL, noted during the drafting of the policy, the UDRP's definition of bad faith differs greatly from the standards set forth in federal law.[61] In practice, the UDRP's definition of bad faith is significantly broader than its ACPA counterpart, and does not allow any of the safe harbor provisions available under the ACPA. Because the UDRP definition requires a harsh, "all or nothing approach" to dispute resolution,[62] complainants are often encouraged to "forum shop" in order to find the court most favorable to the circumstances of their case. This results in an unfair advantage for the complainant.[63] The second problem with the bad faith definition relates to the

---

[59]UDRP, *supra* note 29, § 4(a).

[60]*Id.* at § 4(b). "[T]he following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith: (i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or (ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or (iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or (iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location." *Id.*

[61]ICANN has archived all suggestions made by providers relating to the UDRP on the ICANN website. AOL's comments are *http*://www/icann.org/comments-mail/comment-udrp/current/msg00111.html (last visited September 24, 2005) (on file with the North Carolina Journal of Law & Technology).

[62]*See* Hildenbrand, *supra* note 30, at 642.

[63]Registering a domain name binds that person to use the UDRP at the beginning of a dispute, but it does not bind the party who is making the complaint. It is the complainant's choice where to pursue the dispute. For a full discussion of the effect of forum shopping on domain name disputes, *see* Emerson, *supra* note 9, at 184-195.

remedies available under the Policy. Specifically, UDRP arbitration is not binding.[64] This encourages the losing party to appeal the judgment in federal court, where the differing standard for bad faith could result in a completely different decision.[65]

Under the UDRP, the only remedies available to a complaining party are the cancellation or transfer of the domain name.[66] The limited nature of these remedies indicate that ICANN meant for the alternative dispute resolution ("ADR") methods used under the UDRP to apply to those cases in which the dispute in question did not involve cyberpiracy, or where cyberpiracy was involved but the parties involved wished to bypass the time and expense of federal litigation and simply by correcting the situation at hand.

Realizing, however, that some disputes might require both the speedy recovery of a domain name and damages or criminal prosecution, ICANN purposely drafted the UDRP to allow for concurrent and subsequent litigation.[67] Commentators have argued that what seemed like a good idea at the time of drafting has not worked out well in practice.[68] As mentioned above, it is well settled that the ADR conducted under a UDRP is not binding in federal courts.[69] The obvious effect of this is that parties unhappy with UDRP judgment can re-file in a district court, thus leading to seemingly unending litigation and defeating the purpose of a cost-effective dispute resolution. Equally troubling is the fact that courts sometimes hold that a party must exhaust UDRP remedies before seeking injunctive relief through the courts.[70] The collective

---

[64] *See, e.g.*, Dluhos v Strasburg, 321 F.3d 365, 369-370 (3d Cir. 2003) (holding that UDRP cannot be considered arbitration because it allows parties to file suit before, after, or during the ADR).

[65] Additionally, it has been said that the UDRP has created "procedures that have systematically favored intellectual propriety owners even in doubtful cases." Travis, *supra* note 11, at 32.

[66] UDRP, *supra* note 29 at § 4i.

[67] UDRP, *supra* note 29, at §§ 4-5.

[68] Emerson, *supra* note 9.

[69] *See, e.g.*, Dluhos v. Strasberg, 321 F.3d 365, 369-370 (3d Cir. 2003).

[70] *See, e.g.*, Am. Girl, LLC v. Nameview, Inc., 381 F. Supp. 2d 876, 883 (E.D. Wis. 2005) (denying an injunction where plaintiffs had not pursued action under the UDRP).

effect of these problems seems to be that ADR under the UDRP is "nothing more than an expensive prologue" to litigation.[71]

IV. ICM'S PROPOSED REGISTRATION PROCESS FOR THE .XXX DOMAIN

Despite the limitations of the federal cybersquatting laws and the UDRP, the proposed registration process for the .xxx domain should protect most mainstream businesses and individuals from cyberpiracy.[72] ICM relies on "four principle mechanisms: contractual representations, charter verification, the UDRP, and the Start-Up Trademark Opposition Proceeding ("STOP")."[73] While no registration process can be completely foolproof, the steps outlined by ICM integrate all of the screen processes which have been effective in the past, offering potential victims of cyberpiracy more protection than ever before.

Currently, all people who register a domain name must sign a release that states that they have no reason to believe that they are infringing on anyone's personal mark, that they do not know of any person or business with an interest in the mark, and that they are acting in good faith by registering the domain name.[74] After that step is complete, the domain name information is entered into a *whois* database, which contains information on all domain names within a TLD.[75] As one of its efforts to protect the rights of others, ICM proposes requiring a release to be signed at registration and again when the domain name is registered is with a *whois*.[76]

ICM also intends to utilize "charter compliance" to prevent cyberpiracy. As ICM intends the .xxx domain to be a virtual "red

---

[71] Emerson, *supra* note 9, at 184-95.

[72] .xxx Application, *supra* note 16 at § C Assurance of Community Standards.

[73] .xxx Application, *supra* note 16.

[74] Clark, *supra* note 10, at 1486.

[75] *See, e.g.*, Am. Girl, 381 F. Supp. 2d at 879 n.2.

[76] The registration release requirement will not have much effect on the public, but it appeals to ICANN because it appears to add even greater protection against liability for ICANN and ICM.

light district"[77], the charter insists that every website in the .xxx domain must contain adult content, and ICM has outlined a specific screening process for making sure this requirement is met.[78] ICM asserts that because the domain will contain only sexual content, consumers will recognize the .xxx tag and not confuse the domain names with mainstream businesses.[79] Nonetheless, ICM has recognized that some individuals and businesses will still be concerned about the risk of any association with the .xxx domain. Thus, ICM will offer a "sunrise" period before registration for the TLD opens to the adult entertainment industry. [80] This means that the interested parties can protect their names and trademarks before registration becomes open to the general public.

Another step protecting trademark holders from cyberpiracy is the implementation of a STOP proceeding.[81] STOP is basically a proceeding that halts an abusive registration of a trademark while the registration is still taking place.[82] Essentially, it provides a timely mechanism that ensures that no damage is done to the trademark.[83] STOP proceedings were used with success by

---

[77]"Red light district" is the term consistently used by the media and on the Internet to describe the services that the .xxx will provide.

[78]For a description of how charter compliance will be enforced, *see* .xxx application, *supra* note 16, at Policy Considerations, § C(1)(b).

[79]As Ron Jeremy, the so-called "ambassador of porn" remarked, "xxx" has always been associated with main-stream pornography. *See* Rebecca Breeden, *Porn Star, Christian Debate Adult Film Industry*, 2theadvocate.com, Sept. 29, 2005, http://www.2theadvocate.com/stories/092905/new_porn001.shtml (last visited October 13, 2005) (on file with the North Carolina Journal of Law & Technology).

[80] .xxx application, *supra* note 16, at Policy Making Process § B.

[81] *Id.*

[82] .xxx application, *supra* note 16, at Policy Making Process § C(1)(d).

[83]ICM claims that STOP proceedings will be especially "responsive to the needs of the adult-entertainment community." .xxx application, *supra* note 16, at § D(2). The reasoning behind this declaration involves 15 U.S.C. § 1052(a) (2000), a section of the Lanham Act, which "bars the registration of immoral or scandalous matter on the Principle Register. Moreover, the refusal to register immoral or scandalous matter has been found not to abridge First Amendment rights." .xxx Application, *supra* note 16, at § D(2). While it is clear why the statute is particularly important in light of the content on .xxx, it is not immediately clear why this meets the needs of the adult entertainment

Neulevel during the initial registrations of .BIZ,[84] and ICM believes they can improve on that by slightly extending time period for a STOP proceeding.[85]

For disputes that do not occur during the registration process, ICM will utilize the UDRP.[86] As discussed above in Part III, subsection C, the UDRP can be an inadequate barrier against cyberpiracy and an ineffective means of settling domain disputes. How this will play out in the adult entertainment context will be discussed later in this comment.

Finally, ICM hopes to prevent cyberpiracy by making registration with the domain considerably more expensive.[87] While a price increase in per-domain-name registration may prevent mass registrations of domain names, it seems unlikely that a price hike will prevent an opportunistic cyberpirate from taking advantage of an unclaimed name.[88] Other registration procedures, including the sunrise period for trademark holders and requirement of charter compliance, will probably be more effective at preventing cyberpiracy than a modest price increase.

V. THE ALLURE OF .XXX TO ADULT ENTERTAINMENT COMPANIES

Currently, online adult entertainment is a profitable business without an .xxx domain, and there are no laws or instruments in

---

community. From a common sense perspective, it would seem to aid those wishing to prevent the registration of adult content rather than those trying to provide it.

[84]As proof of the success of Neulevel's STOP proceeding, ICM estimates that roughly one STOP challenge was filed for every seventeen challenges under different sunrise mechanisms. *Id.* at § D2.

[85]STOP proceedings were used by NeuLevel during the "roll-out" phase of .BIZ. ICM proposes a version of STOP that is based on NeuLevel's version with modifications to the timing of notification: "specifically, the notice will be incorporated into a 2-tier both during the initial registration process and during the subsequent whois verification procedure prior to the domain name being added to the zone files for global resolution." *Id.* at § D2.

[86]*Id.* at § C1c.

[87]*Id.*

[88]As of the writing of this article, no specific figure had been made public.

place that would require adult sites to move to the new "red light district."[89] This poses the question of why, if adult sites have already built up customer goodwill, they would want to move to a new domain. The answer, as ICM sees it, has to do with "The Truth in Domain Names" provision of the "Protect Act."[90]

In 2003, Congress passed a forty-seven page bill aimed at preventing child exploitation called "The Protect Act."[91] One provision of the bill[92] requires that websites containing obscene or erotic adult material must not have misleading names. For example, "snowwhite.com" cannot depict a woman fornicating with seven little people.[93] This "Protect Act" is the only federal law to directly touch typosquatting. It was intended to prevent situations typical of cases like *American Girl v. Nameview, Inc*, where a typosquatter registered "amercangirl.com" and linked it to a pornographic website in order to lure children away from a popular toy and book site.[94] However, it applies with equal fervor to adult sites which have a generic or non-sexual term as a domain name.

Unquestionably well intentioned, the "Protect Act" protects children, but deprives adult sites of legitimate marketing options. Like almost every other industry, a handful of big names dominate the adult-entertainment world.[95] However, the privacy and accessibility of online adult-entertainment has fueled consumer demand for content that is well beyond what mainstream "mega-brands" such as Playboy provide. Largely by copying the business plans of these successful "mega-brands," many smaller companies

---

[89]Wagner, *supra* note 4.

[90].xxx application, *supra* note 16, at Policy Making Decisions § C(2).

[91]*See* 18 U.S.C. § 2252B (2000). For a full discussion of The Protect Act and whether it will actually protect children, *see* Kosse, *supra* note 12.

[92]18 USC § 2252B.

[93]While some sites, such as girls.com, continue to post adult content under a misleading name, many sites, such as whitehouse.com, are no longer up.

[94]381 F. Supp. 2d 876 (E.D. Wis. 2005).

[95]*Id.* Interestingly, the defendant in American Girl had registered the domain name anonymously and was nowhere to be found when the case was litigated. This calls into question whether legislation of misleading domain names is really enough to protect children from online pornography.

have become profitable by appealing to a particular look or fetish.[96] Often, adult websites attract visitors by using generic terms, such as "college girl," to describe their sexual content. In addition, Internet entrepreneurs prefer concise domain names, because consumers are more likely to find and return to a site that has a short, easily remembered name.[97] Understandably then, many adult sites would prefer a short domain name containing only generic terms. Unfortunately for adult-entertainment companies, children frequently stumble upon these memorable domain names.[98] Thus, the law forbids adult companies from using them.[99]

From a child-protection standpoint, the advantage of the .xxx domain is literally the .xxx tag. Because .xxx is a well known indicator of adult content, and because the entire domain will, in essence, be known as a virtual "red light district," ICM hypothesizes that generic second level domain names will not be considered misleading under the terms of the Protect Act.[100] Specifically, "ICM and IFFOR[101] [International Foundation For Online Responsibility, hereinafter "IFFOR"] believe that registrants may be better positioned to use an affirmative statutory defense in connection with prosecution under [the Protect Act]."[102] Thus, adult entertainment webmasters who choose to register a .xxx site will have the benefit of a short, descriptive, and easy to

---

[96] Abram Sauer, *How is Porn Penetrating the Mainstream Market?*, Brandchannel.com, March 1, 2004, http://brandchannel.com/features_effect.asp?pf_id=199 (last visited October 12, 2005) (on file with the North Carolina Journal of Law & Technology).

[97] *See, e.g.*, Pure Imagine, Inc. v. Pure Imagine Studios, Inc., No. 03 C 6070, 2004 WL 2967446, at *13 n.8 (N.D. Ill. November 15, 2004) (accepting testimony of defendant that website owners want short names because they are easy to remember as general knowledge).

[98] According to Susan Hanley Kosse's article on Internet pornography laws that protect children, 25%-45% of children using the Internet had unintentionally visited a pornographic website in 2004. Kosse, *supra* note 13, at 38 U. RICH. L. REV. 722 (2004).

[99] 28 U.S.C. § 2252B (2000).

[100] .xxx application, *supra* note 16.

[101] IFFOR is a Canadian nonprofit organization founded by ICM to implement the .xxx TLD. .xxx application, *supra* note 16.

[102] .xxx application, *supra* note 16, at Appropriateness of Sponsored Community.

remember domain name, while, hopefully, remaining free from prosecution.

VI. THE UNREALIZED DANGER OF THE .XXX TLD

As discussed earlier, ICM has carefully considered how to protect mainstream businesses, trademark holders, and individuals from cyberpiracy. Far less thought has gone into the protection of adult entertainment businesses. None of the steps taken to prevent and adjudicate cyberpiracy and domain name disputes within the TLD apply to the adult entertainment industry.

A. *Cybersquatting in .xxx*

ICM's .xxx application procedure takes for granted the fact that cybersquatters might buy the second level domain name of an already existing .com adult site. There seems to be an unstated premise in the ICM application that, since most cyberpirates link the domain names to pornographic websites, cybersquatting cannot exist when all the sites in the TLD feature adult content. This is flawed logic. Cyberpirates do not hijack domain names to flood the Internet with pornography, they do it to extort money. Adult entertainment companies are just as vulnerable to cybersquatting in the .xxx realm because they are not protected by ICM's anticyberpirate screening procedures. Because these sites are seldom trademarked, the majority of them are prevented from registering before the public. The requirement for charter compliance will likewise not protect adult sites, because it only requires that the person registering the .xxx name intends to provide adult content on the site.[103] This merely allows the competition to gain control of a valuable domain name.

The contractual representation policy outlined by ICM is the only mechanism that could prevent this kind of activity. Basically, the policy consists of a release that the registrant must sign indicating that they are registering in good faith.[104] Realistically,

---

[103] .xxx application, *supra* note 16, at C. (referring to Assurance of charter-complaint registrations and avoidance of abusive registration practices).

[104] .xxx application, *supra* note 16, at C.

this policy does not do much besides shield ICM and ICANN from liability. If a party actually intends to register a domain name with the hopes of extorting money from another site, there is no reason to believe why they would have reservations about lying about those intentions. Because successful cyberpirating requires forethought and planning, it is reasonable to conclude that cyberpirates are well aware of the potential consequences of their actions and choose to act anyway. It is unreasonable, however, to think that mere contractual obligations are going to deter domain name hijacking.

Of course, adult websites are welcome to take advantage of the federal courts and the UDRP in order to resolve these kinds of disputes. But adult websites must consider whether they want to resort to high-priced litigation to settle the dispute. Adult entertainment companies, therefore, are left with several uncomfortable options. If they leave their domain names exposed to cyberpirates, (1) they will likely have to contend with expensive, uncertain litigation; (2) they will have to deal with a loss of business resulting from the new site; or (3) they will have to pay off the cyberpirates. Alternately, they can choose to register with .xxx, (a preemptive strike against cyberpiracy) and acquire a domain name they neither need nor want. Cyberpirates, no doubt, will bank on the fact that it is probably cheaper to pay a ransom for the domain name than to litigate the dispute. By contrast, ICM probably hopes that many adult entertainment companies will preemptively register with .xxx in order to prevent a dispute. In effect, adult entertainment companies face a dilemma: pay ICM now, or pay third parties later.

B. *Typosquatting*

ICM similarly has an unrealistic view of typosquatting disputes in the .xxx domain. As the application itself states, "it is highly unlikely that an Internet user will fail [sic] prey to a typo-squatter in the proposed TLD, as it is very unlikely that an Internet user will accidentally type in a second level domain name followed by the TLD extension .xxx."[105] In a limited sense, this is true. It is

[105] *Id.* at § C(4).

unlikely that someone will type in a name of a legitimate business followed by .xxx. However, it is not unlikely for an Internet user to type in "collgegirl.xxx" when they meant to type in "collegegirl.xxx." The result of this mistake will probably not negatively effect the consumer, as both sites would presumably offer similar content. The effect on the businesses involved, however, could be significant.

It seems to offend notions of equity to allow one company to profit from another's work and reputation simply because the consumer made a spelling error. On the other hand, there does not seem to be a clear legal remedy to correct this problem. The aggrieved company could file claims under the federal laws or the UDRP, but the outcome of such cases is uncertain because the domain names in question are not technically trade or service marks. Federal law indicates that the test should examine who used the name in commerce first,[106] but this question is convoluted by the fact that the situation involves two separate domain names, neither of which is necessarily the name associated with the business who owns the website.

Even if the company did have a strong case under either federal law or the UDRP, it still has to balance litigation costs against the value of the business lost. Small companies might bring in less profit by allowing a typo squatter to sponge off their domain name, but they may be unable to stay in business if they pursue litigation.

Typosquatting is especially problematic in this context because it is nearly impossible to prevent. Ostensibly, a company could figure out the most common misspellings of their name and then register each of the possibilities. Ironically, one of the "safeguards" of the proposed .xxx domain is an elevated registration fee.[107] Designed to prevent cyber and typosquatters from amassing many names, the fee increase will likely be more

---

[106]See, e.g., Pure Imagine, Inc. v. Pure Imagine Studios, Inc., No. 03 C 6070, 2004 WL 2967446, at *10 (holding that the controlling factor in the case was the fact that plaintiff had registered the domain name as a trademark, the court suggested that if this was not the case, it would look to who used the name first in commerce).

[107] .xxx application, *supra* note 16.

effective at preventing legitimate domain name holders from registering variations of their names than it will be at deterring cyberpirates from targeting specific businesses.

C. *Generic Term Domain Names in the .xxx*

For reasons described above, generic second level domain names can be a very valuable tool for online adult entertainment businesses. The question then becomes which companies will gain the rights to generic terms. The straightforward answer, and one that ICM seems to advocate, is to offer the names on a first come, first served basis.[108] Nonetheless, the situation cannot be resolved so simply. Take, for example, the generic term "bunnies." In the .xxx context, this term could refer to multiple businesses, including, but limited to, mega-brands such as Playboy, well established brothels such as The Bunny Ranch, websites run by individuals named Bunny, a variety of strip clubs throughout the United States, and possibly even websites dedicated to rabbit fetishes. All of these companies have a legitimate business interest in the name and all would be using the name in good faith. Yet no one actually holds the rights to the name, as federal law does not allow generic terms to be trademarked.[109]

Under the federal laws, it is not clear which, if any, of the businesses interested in bunnies.xxx have a strong case, since none hold a trade or service mark by that name. At the same time, this is not going to prevent interested parties from filing suit in federal court. Because a larger company will be able to afford better lawyers and more legal expenses, it is hard to believe that a relatively small company could ever prevail in a lawsuit, even if that company registered the name first and/or had the strongest interest in the name.[110] Because UDRP disputes are so open ended, a large company could easily begin with a UDRP proceeding and

---

[108] .xxx Application, *supra* note 16.

[109] *See, e.g.*, Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763, 767-768 (1992) (holding that generic trademarks are not subject to trademark protection).

[110] *See* Travis, *supra* note 11, at 5 (noting that when "faced with objections by large corporations and their corporate counsel, small Internet 'typically agree to shut down their sites or remove offending material.'").

then appeal to the federal courts until a favorable result was reached or the other party was forced to settle because of mounting legal fees.

In a dispute where the companies are more evenly matched (and for whom the UDRP looks most attractive because of its relative speed and lower cost), it is not clear who would prevail in the dispute. The first criteria examined in a UDRP proceeding is whether the complainant has a trademark or service rights identical or confusingly similar to the contested domain name.[111] In previous UDRP proceedings, the fact that neither party has trade or service rights in the name was cause to find for the defendant. However, .xxx cases are going to have a different fact scenario. It is entirely possibly for both companies to have a legitimate interest in the name. At the same time, it may have previously been impossible to register the name as a trademark or a domain name. In such a scenario, one would hope than an arbitrator would overlook this particular criterion, as not doing so would automatically also result in a default judgment for the defendant, regardless of any other consideration.

The problem with disregarding the first criterion is that the other criteria, bad faith and lack of legitimate interest, are essentially equally balanced against each other. Bad faith is evidenced by the "purpose of disrupting the business of a competitor; or . . . [an intentional attempt] to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark."[112] Assuming the sites offer similar material, it would be easy for the complainant to prove bad faith. On the other hand, there is a legitimate right to the domain name if the defendant uses it for a bona fide offering of goods and services or "without intent for commercial gain to misleadingly divert consumers."[113] Again, if the businesses sell similar products, legitimate rights should not be difficult to prove. Because the two remaining criteria essentially end the dispute in a draw, it is not

[111] *See* UDRP, *supra* note 29, at § 4a(i).
[112] *See* UDRP, *supra* note 29, at (b).
[113] *See* UDRP, *supra* note 29, at (c).

clear how or by what standards a UDRP .xxx decision will be reached.

VII. CONCLUSION

If .xxx is approved, there are several steps that can be taken which will minimize cyberpiracy and domain name disputes:

A. *Cybersquatting*

To address the problem of cybersquatting, ICM can open the sunrise registration period to adult entertainment sites already in existence, permitting them to register names with .xxx that are identical to those they hold with .com and other domains. A similar process will be utilized when .EU registration opens up.[114] The sunrise period of the .EU will take place in two phases: the first includes registered trademark holders; the second includes any trademark holder who did not choose to register in the first phase, as well as anyone who holds a domain name under a different TLD. In order to qualify for the second phase, the new domain name must be identical to the former domain name. Documentation must be provided to prove that the domain names are identical and are in fact owned by the same person.[115] If the companies chose to take the risk of not registering, they would do so at their own risk.

Another alternative would be for ICM to allow adult entertainment websites to automatically transfer existing domain names on other TLD's to the .xxx domain; doing so would definitely make cybersquatting more difficult. Unfortunately, it might also result in a large loss of revenue to ICM, making it a far less likely possibility.

---

[114] Domainregistry.de, ICANN-Registrar: Pre-registration of EU-domains, https://www.domainregistry.de/edu.html (last visited Nov. 21, 2005) (on file with the North Carolina Journal of Law and Technology).

[115] ICANN-Registrar: Pre-registration of eu-domains, https:// www.domainregistry.de/eu.html (last visited Nov. 6, 2005) (on file with the North Carolina Journal of Law and Technology).

B. *Typosquatting*

To help prevent typosquatting, ICM could waive or lower the registration fee for similarly spelled or misspelled variations at the time the principle domain name is registered. This would allow companies burdened with financial concerns to at least have the choice of protecting the domain name.

C. *Generic Terms*

ICM should take two steps to correct the problems with domain name disputes involving generic terms. First, it should disallow the filing of prior, concurring, and subsequent lawsuits if there are to be UDRP proceedings. This will create a stronger UDRP, as it will then fulfill the federal requirements for arbitration, and it will prevent large companies from using the UDRP to run up legal bills. Second, ICM should draft its own criteria as to how UDRP disputes are to be decided. The criteria should reflect the fact that most of the names in the .xxx are not trademarked, and are probably not possible to trademark.

The best solution to the .xxx problem is for ICANN to reject ICM's application. There is no need for a .xxx domain. Currently, online adult entertainment is big business.[116] While .xxx does provide some otherwise unavailable marketing opportunities, there is no evidence to suggest that the industry is going to suffer as result of not having an .xxx domain.[117] When the potential dangers to adult entertainment companies are considered, the relative value of the domain seems low. At best, .xxx looks like an attempt by ICM to make a large profit by selling unnecessary domain names.

Further, .xxx will do very little to protect children from exposure to pornography. Migration to the domain would be totally voluntary for adult entertainment companies, and if a

[116]In its TLD application, ICM cites that in 2002, 3.3 billion dollars were spent on online adult entertainment, with Reuters predicting that number would rise to 4.6 billion by 2006. .xxx Application, *supra* note 16, Appropriateness of Sponsored TLD Community.

[117]ICM reports that 80% of *Hustler's* sales are either online or video, and attributes the bankruptcy of *Penthouse* and *Screw* magazines to their failure to provide content online. .xxx Application, *supra* note 16.

company does decide to register with .xxx, there is no mechanism to prevent it from keeping its ".com" domain name. From this perspective, the TLD will do very little to limit pornography on the rest of the Internet. Those who support .xxx because they wish to protect children would accomplish more by supporting something like .kids, which would include only non-offensive, kid-friendly material.